Military Commander and the Law
Major Chris Hobbs, 03-4127

Acts of terrorism committed by, with and/or through cyberspace are not virtual crimes. These are very real crimes perpetrated by very real criminals. Unfortunately, the cyber domain is a highly complex and ambiguous operating environment where crime, warfare and terrorism can and does occur. The policing and prosecuting of cyber terrorists in this complex environment frames some of the most troubling aspects of the matter. What is the nature of the crime and who are the victim/s? Who committed the crime? Where did the crime take place? Who has jurisdiction? Are there applicable laws in place to deal with the situation? At times, it seems that there are many more questions than answers. Military counterterrorism efforts and legal institutions can and must be updated and applied to crimes that occur in and through the virtual realm. To this end, two areas are explored in this paper: current U.S. policy commitments and the possibilities and realities of implementing punitive actions against cyber terrorists. The purpose of this paper is to offer a brief overview of how cyber terrorism can be tempered by cyber law in both the virtual domain as well as through conventional means.

Via cyberspace, individual or state-sponsored terrorists are potentially able to affect the Diplomatic, Information, Military and Economic (DIME) instruments of power of target states. In the past decade, the United States Government has began to fully grasp the urgency of the situation presented by cyber terrorism and has issued a plethora of high-level guidance (national strategies, directives, plans and orders) that supports securing cyberspace as a subset of critical infrastructure as a matter of national strategic importance.[1] "In the National Strategy for Homeland Security, the National Strategy to Secure Cyberspace and the National Infrastructure Protection Plan, DoD is identified as the lead Sector Specific Agency for securing the United States cyberspace for the Defense Industrial Base critical infrastructure."[2] Recently, the Secretary of Defense established a subordinate command that will focus exclusively on military

cyber security. The new U.S. Cyber Command will report to the U.S. Strategic Command. Deputy Defense Secretary William J. Lynn, III, noted, "Just like our national dependence, there is simply no exaggerating our military dependence on our information networks: the command and control of our forces, the intelligence and logistics on which they depend, the weapons technologies we develop and field – they all depend on our computer systems and networks. Indeed, our 21st century military cannot function without them."[3] While the DoD has taken the lead for military networks, there remains a valid requirement for several domestic agencies such as the Department of Homeland Security, Department of Justice and the Department of Commerce to work in concert with each other and also with their counterparts in the international community. For instance, within the framework of the United Nations, both the International Law Commission (ILC) and the International Court of Justice (ICJ) play pivotal roles in establishing and prosecuting international laws concerning cyber terrorism.[4] Both internal and external cooperation amongst empowered entities is an essential tenet of cyber justice.

With national leadership recognizing the imminent threat posed by cyber terrorists, it is important to understand what can be done both reactively and proactively to avert future disaster at the hands of cyber criminals. Crime prevention is the first key step in combating any crime. In an effort to defend U.S. critical infrastructure and guard susceptible cyberspace access from potential cyber terrorists, the Department of Defense has taken defensive countermeasures to protect national security interests. "Today, DoD has built layers of defense across the services focused primarily on network access points that allow a 24-hour watch of all critical network operations. Use of security routers, intrusion detection systems (IDS), and certification of systems programs, as defensive measurers greatly restrict an outside agent from hacking his way

into the DoD infrastructure. These technologies help the system administrator's monitor all outside activity thereby gaining a certain amount of situational awareness that alerts them to possible intrusions or attacks."[5] A proactive cyber defense can greatly assist in the protection vital national security interests.

With the military taking the lead for a preponderance of cyber monitoring and intelligence collection in both a domestic and international context, there exists the potential for inadvertent breaching of the Posse Comitatus Act. To help negate this potential problem, the Military Cooperation with Law Enforcement Officials Act was established in1981. Summarizing the assistance that the military can provide to civilian law enforcement in United States v. Johnson[6] "…the military can provide to civilian law enforcement agencies without running afoul of the Posse Comitatus Act… The legislation attempted to maximize the degree of cooperation between the military and civilian law enforcement "in dealing with drug trafficking and smuggling while maintain[ing] the traditional balance of authority between civilians and the military"[7]… The Act permits the Secretary of Defense to "make available any equipment… base facility, or research facility of the Department of Defense to any federal, state, or local civilian law enforcement official for law enforcement purposes."[8] More recently, "the War on Terror has raised questions regarding the domestic aspects of military operations – specifically, the proper delineation of homeland defense from homeland security. In general terms, homeland defense is the domestic use of military forces against foreign enemies, and homeland security includes most everything else."[9] While far from simple or clear cut, this legislation does provide at least one avenue for lawful cooperation between military and civilian law enforcement agencies in the combating of cyber terrorism.

In an effort to provide an encapsulated philosophy or ethos for military conduct in combating cyber terrorism, it appears that modern thought on this subject follows customary lines of reasoning: "Short of armed conflict, the values underlying the non-intervention principle should provide a sufficient guide… in times of conflict the time-tested rules of LOAC are sufficient. In considering an information attack one should consider what international obligation the other party has violated, the effect the operation will have on the legitimate exercise by that state of its sovereignty, and whether that effect is proportionate to the end of remedying the violation, taking into account the feasibility of less coercive means."[10] As interpreted, the LOAC may justifiably be applied to acts of cyber terrorism if in accordance with the idea of *jus in bello*. In other words, the punishment must fit the crime. Since the current frameworks for both military non-intervention and the prosecution of war are broad enough to cover cyber terrorism as an operating environment, the legal aspects of this issue can now be examined to fully appreciate the entire cycle of crime and punishment.

Aside from incidents of domestic cyber terrorism which can be investigated and tried in standing local, state and federal courts of law, foreign acts of cyber terrorism fall into a much more convoluted realm. The first issue includes determining attribution for the crime. "Are cyber terrorists state-sponsored, groups, criminals, individuals or some combination of these?"[11] Additionally, traditional physical evidence (witnesses, DNA, fibers) may not be applicable or practical in the cyber environment. Outside of the courtroom, when kinetic retaliation is considered as an appropriate response by a victim state, more rules and questions apply. With relation to military operations, two main questions are posed as a validity test: "(1) Are we at war? (U.N. Charter paradigm, Schmitt Analysis) and (2) If we are at war, what rules apply? (The four basic tenets of treaty law: Discrimination, Necessity, Proportionality, Chivalry.)"[12] Once

past the line of belligerency, a cyber terrorist poses at least two major questions for military cyberspace operators: "(1) which interstate activities in cyberspace constitute a threat or use of force under international law, and (2) when such a threat or use of force does constitute an armed attack under international law, how does the law of armed conflict apply to the lawful exercise of the inherent right of self-defense in cyberspace?"[13] "These questions are fundamental to the law of information conflict (LOIC), which is the composite of the peacetime regime of international law, the law of conflict management, and the law of armed conflict that regulates the conduct of all state activities in cyberspace."[14] Along with these broad guidelines, the "Schmitt Analysis" provides a framework of themes for decision-makers to examine when confronted with an option for which instrument of power best imparts a state's desired strategic response. The "Schmitt Analysis" poses the questions of, "severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy and responsibility"[15] on a state's actions. Pending thorough analysis, the military instrument of power may not be the most appropriate response to a cyber attack. A state may ultimately seek justice by teaming with their international partners that possess jurisdiction in the matter, and leverage more diplomatic, informational or economic tools as opposed to a contemporary military response.

Domestic preparations can hinder the frequency and magnitude of attacks perpetrated by cyber terrorists, but the key to effectively combating determined enemies in the virtual realm goes back to international cooperation between state actors. "International laws are in place to address the ever-changing nature of warfare. The Hague Conventions, the principles of jurisdiction and the territorial sovereignty all provide a framework for addressing all warfare to include cyber warfare operations."[16] "Legal experts can measure cyber warfare operations against existing case studies where the effects are evaluated, as opposed to the means, even if the

operations originated outside the nation's territorial jurisdiction. There is some authority validating jurisdiction over conduct outside state territory "that has or is intended have substantial effect within its territory."[17] "There are three jurisdictional principles that provide nations the right to pursue aggressors that threaten a nation's independence: the Territorial Principle, Nationality Principle and the Protective Security Principle."[18] The territorial principle clearly states that a "state has jurisdiction over all crimes committed in its territory…to include airspace, international waters and territorial seas."[19] In the nationality principle "states may exercise jurisdiction over its citizen…even if they are physically outside the states' territory."[20] Finally, the protective security principle is defined as "a state may assume jurisdiction over, and punish foreign nationals for certain conduct outside its territory, which is directed against its security, territorial integrity and political independence."[21] The United States cannot afford to police the entirety of cyberspace alone. Cyber terrorism is a global problem that requires a global solution.

When viewed as a whole, the issue of combating cyber terrorism through legal channels is a daunting proposition. While the threat is unilaterally accepted as a diabolical new medium for would-be terrorists, both the law enforcement and legal communities are reeling to bring their methods up-to-speed with the technology of criminal actors. Both domestically and internationally, governments have issued policy guidance concerning the matter. While manpower, structure and financial changes to organizations are underway, there also exists both a technology and education gap that hinders the timely realization of desired results. Internationally, the situation is also improving. Continued cooperation between state law enforcement agencies, militaries and legal advocates at this level seems to be the most promising and expeditious course for combating cyber terrorism presently, and in the foreseeable future.

[1] Griffin, "DoD Role for Securing United States Cyberspace," p 10.

[2] Ibid, p 42.

[3] Miles,"Gates establishes New Cyber Command," http://www.defense.gov/news/newsarticle.aspx?id=54890, June 24, 2009.

[4] Moore, "Information Warfare, Cyber-Terrorism and Community Values," p 65.

[5] O'Hara, "Department of Homeland Security Policy for Defense of Cyberspace," p 11.

[6] Brenner, Cyberthreats: The Emerging Fault Lines of the Nation State, p 179.

[7] Ibid., p 179.

[8] Ibid., p 179.

[9] Wingfield and Michael, "An Introduction to Legal Aspects of Operations in Cyberspace," p 14.

[10] Moore, "Information Warfare, Cyber-terrorism and Community Values," p 136.

[11] Brenner, Cyberthreats: The Emerging Fault Lines of the Nation State, p 127.

[12] Wingfield and Michael, "An Introduction to Legal Aspects of Operations in Cyberspace," p 2.

[13] Ibid., p 10.

[14] Ibid., p 10.

[15] Ibid., p 11.

[16] Sinks, "Cyber Warfare and International Law," p 26.

[17] Ibid., p 26.

[18] Ibid., p 15.

[19] Ibid., p 15.

[20] Ibid., p 15.

[21] Ibid., p 15.

REFERENCES

Brenner, Susan W., Cyberthreats: The Emerging Fault Lines of the Nation State, Oxford University Press, New York, NY. 2009.

Griffin, Jane J., "DOD Role for Securing United States Cyberspace," Air Force Institute of Technology, Wright-Patterson AFB, OH. March 2008.

Miles, Donna, "Gates Establishes New Cyber Command," U.S. Department of Defense News Article, http://www.defense.gov/news/newsarticle.aspx?id=54890. June 24, 2009.

Moore, Joe W., "Information Warfare, Cyber-Terrorism and Community Values," Air Force Institute of Technology, Wright-Patterson AFB, OH. January 2003.

O'Hara, Timothy M., "Department of Homeland Security Policy for Defense of Cyberspace," U.S. Army War College, Carlisle, PA. April 2003.

Sinks, Michael A., "Cyber Warfare and International Law," Air Command and Staff College, Maxwell AFB, AL. April 2008.

Wingfield, Thomas C. and James B. Michael, "An Introduction to Legal Aspects of Operations in Cyberspace," Naval Postgraduate School, Monterey, CA. April 2004.